REMARKS

This amendment responds to the office action mailed January 24, 2005**Error! Reference source not found.**. In the office action the Examiner:

- rejected claims 6, 7, 17, 19, 25 and 31 as being indefinite under 35 U.S.C. 112, second paragraph;
- rejected claims 1-5, 8-13, 15-17, 20-29 and 32-36 under 35 U.S.C. 103(a) as being unpatentable over Paunikar et al (US 2004/0073704) in view of Fink et al (US 6,496,935); and
- objected to claims 18 and 30 as being dependent upon a rejected base claim.

After entry of this amendment, the pending claims are: claims 1-36.

Claim Rejections – 35 USC §112

Applicants have amended claims 6, 18, and 30 to clarify that the limitation "the pre-mapping and/or post-mapping parameter domains" corresponds to the limitations "a pre-mapping parameter domain" and "a post-mapping parameter domain" recited in claims 5, 17, and 29, respectively. Applicants have also amended claims 7, 19, and 31 so that they are respectively dependent from claims 5, 17, and 29.

Applicants have amended claims 13 and 25 by eliminating the term "relationship". As a result, the event's network session recited in claims 13 and 25 refers to the one to which the event belongs and which has been recited in the instructions for establishing a correlation in claims 13 and 25, respectively. Applicants have also amended claims 13 and 25 to correct a typographical error. The term "belong" should be "belongs".

No new matter is added with these amendments.

Claim Rejections – 35 USC §103

To establish prima facie obviousness, three basic criteria have to be satisfied:

- The prior art must provide one skilled in the art with a suggestion or motivation to modify or combine the teachings of the references relied upon by the PTO to arrive at the claimed invention.
- The prior art must provide one skilled in the art with a reasonable expectation of success.
- The prior art, either alone or in combination, must teach or suggest each limitation of the rejected claims.

Furthermore, the teaching or suggestion to make the claimed invention, as well as the reasonable expectation of success, must come from the prior art, not Applicants' disclosure.

The Examiner rejected claims 1-5, 8-13, 15, 17, 20-29, and 32-36 as being unpatentable over Paunikar in view of Fink. Applicants respectfully disagree.

A feature shared by Paunikar and Fink is that they both fall into the field of processing data packets individually. As will be explained in more detail below, there is no attempt in Paunikar and Fink to associate one data packet with another one based on their respective packet parameters in either reference.

Using Fig. 3 of Paunikar as an example, a device implementing a network address translation (NAT) scheme first determines if a data packet is outgoing or incoming (step 210). For each outgoing data packet, the device conducts a lookup for a connection corresponding to the packet parameters (step 220). If an existing connection is identified, the device uses it to translate the private IP address of the data packet into a public IP address (step 240); otherwise, the device establishes a new connection for the packet (step 250). Depending on the type of the data packet (step 260), different operations, basic NAT (step 270) or NAPT (step 280), are employed to identify a public IP address for the newly established connection.

For each incoming data packet, the device conducts a lookup for a connection corresponding to the packet parameters (step 290). If an existing connection is found, the device uses it to reverse translate the data packet's public IP address into a private IP address (step 320); otherwise, the system simply drops the packet (step 310).

Similarly, Fink discloses a method for accelerating packet filtration by supplementing a firewall with a pre-filtering module. If a data packet comes from a source previously permitted by the firewall, the pre-filtering module directly forwards the data packet to its destination. Otherwise, the data packet is handled by the firewall. After transferring responsibility for a source to the pre-filtering module, the firewall no longer receives any data packet from this source until a timeout associated with the source occurs, or a data packet is received with particular session-control field values, such that a connection to the source is closed.

In sum, a NAT device or a firewall is able to finish processing of a newly arriving data packet arriving **solely** based on the data packet itself without correlating the data packet with another one. For example, in the event of translating the IP address of an incoming data

packet, there are only two possible outcomes: (1) getting a private IP address if a matching connection is found or (2) being dropped by the NAT device. There is no second chance for the dropped packet to be revisited simply because it may be related to another data packet that has a matching connection.

By contrast, the present invention is a method of grouping multiple network events into a unique network session by examining their respective event parameters, not a method of processing data packets on an individual basis.

As a background of the present invention, when a message associated with a network session travels along a network routing path from a source to a destination, it may trigger security devices deployed along the network routing path to generate multiple network events. These network events clearly all correspond to the same network session. However, the existence of network address translation (NAT) devices on the network routing path often change the parameters associated with different network events (e.g., events E1 and E2 in Fig. 2), making it difficult to directly correlate network events with the network session using their respective event parameters.

Claim 1 of the present invention is directed to a method for discovering the real event parameters of each network event by removing the influence of the NAT devices on the network event and thereby grouping together network events associated with the same network session. For each member in a stream of network events, the method determines if the network event is associated with any existing network session. If not, the method identifies one or more network address translation rules for the network event, and classifies the network event into a particular category based on the identified network address translation rules. At a predefined moment, the method identifies all categorized network events deemed associated with a particular network session, groups these network events into a set, and assigns the set a unique identifier.

In other words, the method according to claim 1 not only processes each network event individually but also correlates one event with another one by examining their respective event parameters after removing the influence of any NAT operations upon them. As a result, even if a network event fails to match any existing network session **initially**, it may be associated with one network session **subsequently** through its correlation with another network event. This feature of inter-event correlation is clearly missing from the two cited references.

In addition, the Examiner's analysis of Paunikar and Fink is based on the incorrect assumption that "network events" are the same as "data packets" or "messages" transmitted through a communication network. This interpretation of "network events" is directly contrary to the requirements of the pending claims. For example, the first element of Claim 1 is:

> receiving a stream of network events, each network event including a set of event parameters in association with a network session that corresponds to a message being transmitted through a network; (emphasis added)

Thus, as required by claim 1, each network event includes information about a message (e.g., a data packet) being transmitted through a network, which clearly indicates that the network events are distinct from the data packets or messages. As explained in the current application, see paragraphs 0006 and 0008, monitoring or security devices generate network events when they detect suspicious data packets or messages passing through the network. Since neither Paunikar nor Fink concern identifying groups of networks events that correspond to a same network session (i.e., a same message being transmitted through a network), these references separately or together do not teach the claimed invention.

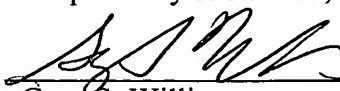
Since Paunikar and Fink, alone or combined, do not teach or suggest the feature of inter-event correlation, claim 1 and its dependent claims 2-12 are patentable over Paunikar in view of Fink.

Claims 13 and 25, and their dependent claims, are patentable over Paunikar in view of Fink for at least the same reasons mentioned above.

In light of the above amendments and remarks, Applicants respectfully request that the Examiner reconsider this application with a view towards allowance. The Examiner is invited to call the undersigned attorney at (650) 843-7501, if a telephone call could help resolve any remaining items.

Respectfully submitted,

Date: April 8, 2005



31,066

Gary S. Williams (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square, Suite 700
3000 El Camino Real
Palo Alto, California 94306
(650) 843-4000